09-11-00

A

Attorney Docket No. 1475B.5A.5

APPLICATION FOR U.S. PATENT TRANSMITTAL FORM

The Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Transmitted herewith for filing is the patent application of:

Inventor(s) Mark E. Ogram

For: A Method of Processing Payment On A Network Of Computers Such As The Internet

[X] Utility [ ] Design [ ] Plant

Enclosed are:

(1) 8 sheet(s) of informal drawings;
(2) Specification with claims;
(3) Application for U.S. Patent, Declaration, and Power of Attorney;
(4) A duplicate copy of this form;
(5) Check Number 3637 for the amount of $385.00
(6) Verified Statement (Declaration) Claiming Small Entity;
(7) Assignment (Including form PTO-1595);and
(8) Disclosure Statement.

Payment is based on the following calculations (37 C.F.R. 1.16):

BASIC FILING FEE ..... $ 345.00

(X) Small Entity @ $345.00
( ) NOT Small Entity @ $690.00

NUMBER OF INDEPENDENT CLAIMS 3
Number in excess of 3: 0 ..... $ 0.00
(X) Small Entity @ $39.00 each
( ) NOT Small Entity @ $78.00 each

NUMBER OF CLAIMS 14
Number in excess of 20: 0 ..... $ 0.00
(X) Small Entity @ $9.00 each
( ) NOT Small Entity @ $18.00 each

NUMBER OF MULTIPLE DEPENDENT CLAIMS 0 ... $ 0.00
( ) Small Entity @ $130.00
( ) NOT Small Entity @ $260.00

ASSIGNMENT RECORDATION FEE ($40.00) ..... $ 40.00

TOTAL: $ 385.00

All correspondence relating to this application may be addressed to the undersigned at:

Mark E. Ogram
8040 S. Kolb Road
Tucson, AZ 85706

Mark E. Ogram
Attorney for Applicant

9/8/00
Date
Reg. No. 30343
(520) 574-3399

CERTIFICATE OF MAILING BY "EXPRESS MAIL"
"Express Mail" Mailing Label No. EL552028422US
Date of Deposit: 9-8-00

I hereby certify that this New Patent Application and Fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Dated: 9-8-00

Sybil H. Tiedemann

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f)) - SMALL BUSINESS CONCERN

As the legal representative of Net MoneyIN, Inc. a corporation under the laws of the State of Arizona, located at 8040 South Kolb Road Tucson, Arizona 85706, I hereby declare that it is a Small Business Concern, as defined in 37 CFR 1.9(d), for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code with regard to the invention entitled: A Method Of Processing Payment On A Network Of Computers Such As The Internet, and filed Contemporaneously.

I further declare that exclusive rights to the invention have been conveyed to and remain with the above identified small business concern.

The Small Business above acknowledges its duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

Signature: ______________ Date: 9/8/00

Name of Person Signing: Mark E. Ogram
Title: Vice President
Address: 8040 South Kolb Road
Tucson, Arizona 85706

A METHOD OF PROCESSING PAYMENT ON A NETWORK OF COMPUTERS SUCH AS THE INTERNET

MoneyIN
Docket No. 1475B.5A.5

"SPEC475B.5A5"

September 3, 2000

A METHOD OF PROCESSING PAYMENT ON A NETWORK OF COMPUTERS SUCH AS THE INTERNET

Background of the Invention:

This is a continuation of United States Patent application serial number 09/400,724, filed on September 21, 1999, and entitled □Financial System of Computers□, which was a continuation of United States Patent application serial number 09/166,749 filed on October 5, 1998, and entitled □Financial System of Computers□, which was a continuation of United States Patent application serial number 08/597,017, entitled □An Improved Financial Transactions System□ filed February 5, 1996, now United States Patent number 5,822,737, issued on October 13, 1998.

This invention relates generally to financial transactions and more particularly to transactions involving credit or debit cards.

The time is fast approaching where a significant amount of commerce will be conducted using distributed networks of computers such as the Internet. The reason this ground-swell of commerce will occur is the ability of a single merchant to economically reach a vast number of potential customers at substantially no costs. Further, the customers are able to review a great number of vendors and their products with the ease of a few key strokes and clicks of the mouse.

Although there are vast numbers of merchants already using such

networks, the sales volume has been particularly low due to a variety of reasons. One reason which has depressed commerce on the networks, is the difficulty with which customers can pay for their purchases.

A variety of techniques have been developed to cure this problem ranging from accepting phone orders to the establishment of another currency called "E-Cash".

Phone orders in response to merchant promotional materials creates a variety of problems. One major problem is the requirements for phone lines and personnel to receive and process the phone orders. Another hurdle is the simple fact that most customers have a single phone line to their residence and this line is used by the computer for accessing the network; the customer has to disconnect from the network to make the phone order.

Although E-Cash is a viable alternative, it is faced with some enormous problems which will be difficult or impossible to address. These include: counterfeiting problems; government reluctance to accept the concept; difficulties in getting access for handling E-Cash; and, the low number of users and merchants which can use E-Cash.

It is clear from the foregoing that there is a need for an efficient methodology and system to accept payment over distributed computer networks.

Summary of the Invention:

The present invention contemplates a totally automated system for securing payment via a distributed network of computers. In this context, the invention creates an automated payment system particularly suited for purchases over a network such as the Internet.

Although the present invention is described relative to the Internet, its application is not so limited and is intended to be used on any distributed computer system in which merchants and consumers interact for the purpose of supplying and purchasing goods or services.

In such a distributed computer network, a merchant or vending computer contains certain promotional information which is communicated to a customer's computer. This information is intended to give the customer sufficient information to make a decision on if the goods/services are acceptable.

As used within this discussion, the term "merchant computer" signifies a computer system which is used for the purpose of selling goods or services. The vendor itself does not necessarily own the computer; in some situations, the computer is operated on behalf of the merchant or vendor.

Based upon the promotional information, the consumer/operator of the customer's computer decides to purchase the services or goods described by the promotional information.

It is at this point where the present invention is particularly powerful as it provides a simple, easy, methodology and linkage for the customer to pay for the goods/services.

In this context, the customer's computer is linked to a payment processing computer and the customer's credit card number and the amount of

the goods or services is transmitted to the payment processing computer. For security reasons, an encrypting software package is first downloaded to the customer's computer so that the credit card number is secure from "hackers" who might also be on the network.

Although the term "credit card" is used, the invention covers the use of any type of financial guarantee card such as automatic debit accounts, checking account numbers, savings account numbers, and other such devices obvious to those of ordinary skill in the art.

The payment processing computer automatically contacts a bank for verification of the credit card and amount; the bank transmits an authorization to the payment processing computer. This authorization, usually in the form of a number, is stored within the payment processing computer's memory for later reference.

The link or connection with the bank is terminated by the payment processing computer and the payment processing computer turns its attention to the customer's computer. The payment processing computer communicates a self-generated transaction indicia, and in some embodiments a password, to the customer's computer.

The transaction indicia is generated by the payment processing computer for proper record keeping. The transaction indicia is also used by the customer to verify that an order has been generated and accepted.

The password is defined by the merchant's computer for the payment processing computer to pass along to the customer's computer. The password is used by the customer's computer to gain access to restricted material within the merchant's computer.

As example, assume the merchant's computer is supplying information as to genealogy. As an initial process, the customer enters the name being researched and receives a preliminary report on the genealogy (the promotional material). To proceed though, and get the actual data, the customer must pay to access this further information.

To do so, the customer links with the payment processing computer, and in the manner outlined above, receives back the transaction indicia and the password. The payment processing computer links the customer computer back to the merchant computer; the customer provides the password to the merchant's computer and is given access to the full genealogy report.

As outlined in this example, in the embodiment where a password is used, the customer's computer uses the password with the merchant's computer in obtaining access to protected information or to establish shipping instructions.

The re-linking of the customer computer to the merchant computer is accomplished in a variety of ways. In the preferred embodiment, the payment processing computer obtains the merchant's address or Unique Recognition Location (URL) from the customer computer when the customer connects with the payment processing computer. This URL is used in a variety of ways, to identify the merchant, to establish the amount of the product/service, and to establish the return URL when the payment processing computer is done with its task for the customer computer.

By selective use of the URL on the merchant's part, the URL transmits a tremendous amount of information to the payment processing computer. As example, assume the URL for the home-page of the merchant is:

http://merchant.com/widget.

When the merchant is selling a single product (a widget), this URL is easy to match to the product. When the merchant wants to sell a variety of widgets, then for a blue widget, the URL might be: http://merchant.com/widget/blue.

In some embodiments, the customer's computer is not linked back to the originating URL of the Merchant computer but rather to another URL. The return URL is stored in the payment processing computer and is used when the Merchant wants the customer/consumer to be passed back to a different location (i.e. where the restricted access information is accessible, or to inform the consumer that their card has been rejected).

The invention, together with various embodiments thereof, will be more fully explained by the accompanying drawings and the following descriptions.

Drawings in Brief:

Figures 1A and 1B are block diagrams of the two computer configurations used in the preferred embodiment.

Figure 1C is a graphical representation of the preferred memory organization for the computer illustrated in figure 1A.

Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the connections and disconnections of the preferred order.

Figures 3A, 3B, 3C, and 3D are frontal views of one embodiment of a consumer's display screen.

Figure 4A is a flow-chart of the preferred embodiment's payment processing operation.

Figure 4B is a flow-chart of an alternative embodiment's payment processing operation.

Figure 5 is a flow-chart of the operation of the merchant's computer.

Drawings in Detail:

Figures 1A and 1B are block diagrams of the two computer configurations used in the preferred embodiment.

Figure 1A illustrates the configuration of the preferred payment processing computer. As shown, computer 10A is a simple layout of a Central-Processing-Unit (CPU) 11A which uses both non-volatile memory 12A and Random-Access-Memory (RAM) 13A.

Communication to and from CPU 11A is via modem 14A which communicates with other computers via the network connected by phone line 15A.

Computer 10B, illustrated in figure 1B, shows the preferred computer configuration used for the merchant computer and the customer computer. Again, CPU 11B is connected to memories RAM 13B and non-volatile memory 12B. In the case of the merchant computer, the promotional material is stored on non-volatile memory 12B and is retrieved and communicated by CPU 11B using modem 14B and phone line 15B.

This system is able to communicate with an operator via monitor 16 for visual information. Monitor 16 is used for the perusal of the promotional material by the customer.

Keyboard 17 is used to communicate operator commands to CPU 11B. In like fashion, mouse input device 18 is also used for operator input to CPU 11B.

Optional printer 19 is used to create a hard copy of the material being displayed to the operator/customer via monitor 16.

The differences between the computers shown in figure 1A and 1B are pronounce since the payment processing computer of figure 1A does not require

input or direction from a human operator. Rather, in the preferred embodiment, the payment processing computer runs totally automatically and collects all of the data and information it requires for its operation automatically from the computers with which it is linked and with what is stored in its memory.

Figure 1C is a graphical representation of the preferred memory organization for the computer illustrated in figure 1A.

Memory 9, located preferably in non-volatile memory 12A, has three sections. The first section 8A is the product listing reference which is composed of multiple groupings. This data remains relative constant and is defined by the merchant. Each grouping, such as 7A, includes data identifying:

- Part Number
- Merchant Identification
- Cost of Product/Service
- Description of the Product/Service
- Authorized Return URL
- Rejected Return URL
- Password

The second section is for defining the merchant's information. Each grouping 7B within section 8B contains relative constant information such as:

- Merchant Identification
- Business Name
- Contact Name within the Business
- Business Address

E-Mail address for the Business

Bank Checking Number for the Business

The third section 8C is an accounting listing which is constantly upgraded as new payments are processed. This section is used for making full accounting to the various merchants. Grouping 7C within section 8C contain:

Transaction Number

Date of transaction

Amount of the transaction

Part number involved in transaction

Credit Card Number

Authorization Number

The authorization number is the indicia received from the bank indicating that the credit card charge has been accepted.

The use of memory 9 allows the payment processing computer to have access to the necessary information to handle the linkage and perform the proper accounting.

Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the connections and disconnections of the preferred order.

Referring to figure 2A, in a typical fashion, a consumer via customer computer 21 enters the network 20 and searches through various merchant computers until the consumer locates the merchant of choice and connects with merchant computer 22. Merchant computer 22 communicates the promotional material via network 20 to customer computer 21.

When the consumer decides to buy the service or product from merchant 22, as shown in figure 2B, the link with merchant computer 22 is broken and

customer computer 21 links with the payment processing computer 23. In the change from merchant computer 22 to payment processing computer 23, an indicia of the URL or the product being promoted by merchant computer 22 is communicated to the payment processing computer 23.

The indicia as a URL of the last site is available through normal network operations and its handling is obvious to those of ordinary skill in the art. The product number is easily combined with the URL; thereby making the product number also available to the payment processing computer 23.

In some embodiments, the originating URL is crossed checked to a memory data base to achieve the product number. In this embodiment, the merchant structures its material so that only a single product/service is associated with a specific URL.

Using the product number (or developing the product number from the merchant's URL), the payment processing computer is able to cross reference its own memory (as described earlier) to achieve other important information including: the amount of the product/service, a description of the product/service, the name and address of the merchant, and other which will be used in later operations.

The payment processing computer 23 accepts from the customer computer 21, the credit card account number which is to be debited the amount of the product.

As shown in figure 2C, in this embodiment, while maintaining linkage with the customer computer 21, the payment processing computer 23 establishes a link via phone lines 25 with the credit card server computer 24. The credit card account number and amount is communicated to the credit card server

computer 24 which responds to the payment processing computer 23 with an authorization indicia. This authorization indicia gives the acceptance or denial of the charge.

If a product is to be shipped, and if the charge has been authorized, as shown in figure 2D, the payment processing computer 23 connects with the merchant computer 22 and directs the merchant to ship the product to the consumer.

As shown in figure 2E, since the payment processing computer 23 has identified the product number, it is able to retrieve from its memory the URL for reconnecting the customer computer 21 with the merchant computer 22. In this manner, the entire operation is totally transparent to the consumer since they feel they have been continuously working with the merchant computer 22.

Further, using the URL's from its memory, the payment processing computer 23 is able to link the customer computer 21 to the merchant computer 22 at an address which is different from where the consumer was originally connected. In this manner, the payment processing computer 23 is able to direct the consumer to different locations which are consistent with the authorization indicia (accept/reject) on their credit card.

As example, assume, the credit card was authorized, then the consumer could be reconnected to an area which has restricted access so that the consumer can gain the information paid for; if on the other hand, the credit card was rejected, the connection would be to a page indicating such and possibly asking for another card number.

In this manner, the payment processing computer 23 is able to control the operation and interface between the customer computer 21 and the merchant

computer 22.

Periodically, the payment processing computer 23 connects via the phone lines 25 with the credit card server 24 and instructs it to transfer the appropriate amount of funds to the merchant's bank computer 26 so that the merchant has access to the funds paid for his product/service provided to the consumer.

Figures 3A, 3B, 3C, and 3D are frontal views of one embodiment of a consumer's display screen.

Screen 30A is designed to provide the promotional information so that the consumer is attracted to purchase the product. In screen 30A is the name of the merchant company (XYZ CO.) 31, the name of the product (widget) 32, the price ($14.95) 33, and the part number (#10234) 34.

Also located on screen 30A is a software key 35 which allows the consumer to pay for the product. In this embodiment, by activating this software key 35 (typically through a click of the mouse), screen 30A is changed to screen 30B which is identical except that the software key 35 has been replaced with an order window 36.

Order window 36 allows the consumer to complete the necessary information to order the product. This includes the part number 37A, the amount 37B, and the credit card number 37C. When the consumer is ready, the software key "Send" 37D or the software key "Cancel" 37E is activated. In the case of a cancel, the screen returns to screen 30A.

In a "send" 37D, mode, the payment processing computer contacts the bank computer and determines if the credit card is valid and if the amount is available. If the charge is authorized, the screen changes to 30C in which

the order window 36 has been replaced with authorization window 38 which shows that the charge has been accepted 39A, the transaction no. (A1483) 39B, and the password ("GO") 39C which the consumer is to use with the merchant.

When this information has either been printed or committed to memory, the consumer activates software key 39D to "Proceed" to screen 30D. At this point, the consumer is able to enter the password 29 so that the restricted access is lifted. In the genealogy example, it is at this point the consumer gains access to the full report.

Figure 4A is a flow-chart of the preferred embodiment's payment processing operation.

After start 40A, a connection is made with the customer computer 41A and the encryption software is downloaded to the customer computer 41B. Encryption software is preferably used for transmittal of the credit card number so that the integrity of the card is not jeopardized.

The consumer computer then communicates, and the payment processing computer accepts, the account number, the amount, and the identification of the product or service, 42A. A connection is made with the credit card server 41C and the account number and amount is transmitted 41D to the credit card server over the established phone lines. In response to this query, the authorization data is received 42B and the connection with the credit card server 41E is broken.

A transaction indicia is generated 41F. This transaction indicia is not the authorization data but serves as an internal monitoring system for the payment processing computer so that the accounting is kept accurate.

From the memory, the password is withdrawn 41G for the product so

ordered; and, the password and transaction indicia is transmitted to the customer computer 41H.

At this point, the connection with the customer computer is terminated 41I and the program stops 40B.

Figure 4B is a flow-chart of an alternative embodiment's payment processing operation.

After start 43A, the program connects with the customer computer 44A and at the same time obtains the merchant URL 45A. Using the merchant URL, the payment processing computer searches its memory and identifies the merchant number, the part number, and the purchase amount 44B.

The encryption software is downloaded into the customer computer 44C and the credit card account number is received 45. A connection is then made with the credit card server computer 44D and the account number and the amount is transmitted 44E. This inquiry results in an authorization code 45C being received and the connection with the credit card server being broken 44F.

A check is then made to see if the credit card purchase was authorized 46A.

If the credit card purchase was denied, the URL to use for a rejection is withdrawn from memory 44G and the Customer computer is connected to the merchant computer at this URL 44H leaving the payment processing computer able to disconnect 44I and stop 43B.

Should the credit card purchase be accepted, 46A, then the program generates a transaction identification 44J. This transaction identification is stored along with the date, amount of purchase, and the merchant number 44K.

The password is retrieved from memory 44L and it, together with the transaction identification, is transmitted to the customer computer 44M.

From memory, the authorized URL is withdrawn 44N.

A determination, based upon stored data, is made as to the character of the product (service or goods) 46B. If the product relates to goods which are to be shipped, a shipping order including the transaction identification, the amount, the date, and address of the customer, is communicated to the merchant 44O to satisfy the order. If the product is a □service□, the program skis to step 44P.

The customer computer is then connected to the authorized URL 44P and the connection with the customer computer is terminated 44Q allowing the program to stop 43C.

Figure 5 is a flow-chart of the operation of the merchant's computer.

After start 50A, the merchant computer connects with the customer computer 51A and communicates the promotional material 52A. The password is received from the customer 52B and is checked to see if it is the correct password 53A.

If the password is incorrect, a determination is made on if it is the customer's first try 53B; if it is, then the customer is given another chance to enter the correct password 52B. If the customer has tried twice to enter the correct password, the connection with the customer is terminated 51C and the program stops 50C.

If the password is correct, 53A, then the secure or restricted access data is communicated to the customer's computer 51D and the connection with the customer's computer is terminated 51B. The program then stops 50B.

In this manner, secure information is selectively transmitted to a customer's computer upon the presentation of a password.

It is clear from the foregoing that the present invention creates a highly improved system for acceptance and processing of payments over a distributed computer network.

What is claimed is:

1. A method of operating a computer on a network comprising the steps of:

a) receiving customer account data and amount data from a remote computer via said network;

b) based upon said account data and said amount data, establishing an authorization indicia; and,

c) communicating said authorization indicia to said remote computer via said network.

2. The method according to claim 1, further including the step of communicating a password to said remote computer.

3. The method according to claim 2, wherein the step of communicating a password includes the step of sending the password via said network.

4. The method according to claim 1, wherein the step of establishing an authorization indicia includes the step of communicating said account data and amount data via a phone network.

5. The method according to claim 4, wherein the step of establishing an authorization indicia includes the step of receiving an acceptance indicia via said phone network.

6. A method of processing a payment order over a network comprising the steps of:

a) receiving customer account data and amount data via said network;

b) based upon said account data and said amount data, establishing an authorization indicia; and,

c) communicating said authorization indicia to a remote computer via said network for the satisfaction of said payment order.

7. The method according to claim 6, further including the step of communicating a password to a second remote computer.

8. The method according to claim 7, wherein the step of communicating a password includes the step of sending the password via said network.

9. The method according to claim 6, wherein the step of establishing an authorization indicia includes the step of communicating said account data and amount data via a phone network.

10. The method according to claim 9, wherein the step of establishing an authorization indicia includes the step of receiving an acceptance indicia via said phone network.

11. An Internet payment processing method comprising the steps of:

a) receiving customer account data and amount data from a remote computer via said Internet;

b) based upon said account data and said amount data, establishing an authorization indicia indicative of payment compliance; and,

c) communicating said authorization indicia to said remote computer via said Internet.

12. The method according to claim 11, further including the step of communicating a password to a second remote computer.

13. The method according to claim 12, wherein the step of communicating a password includes the step of sending the password via said Internet.

14. The method according to claim 11, wherein the step of establishing an authorization indicia includes the steps of:

a) communicating said account data and amount data via a phone network; and,

b) receiving an acceptance indicia via said phone network.

Abstract:

A method of operating a computer on a network of computers for the purpose of collecting payments due a remote computer on the network (such as the Internet). The method for payment processing includes the steps of: receiving the customer□s account data and amount data; establishing an authorization indicia; and, communicating said authorization indicia to a remote computer (such as the merchant□s computer) on the network.

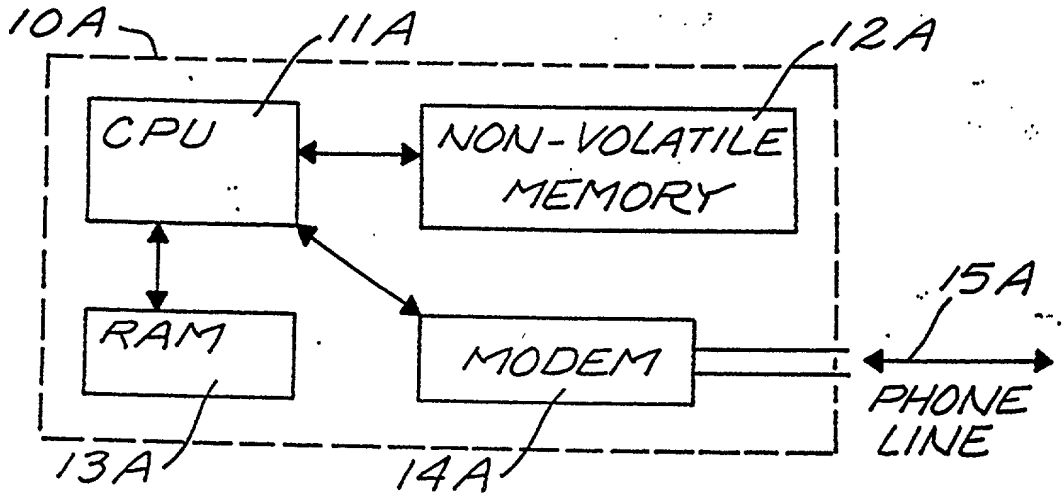

10A
11A
12A
CPU
NON-VOLATILE MEMORY
RAM
MODEM
15A
PHONE LINE
13A
14A

FIG. 1A

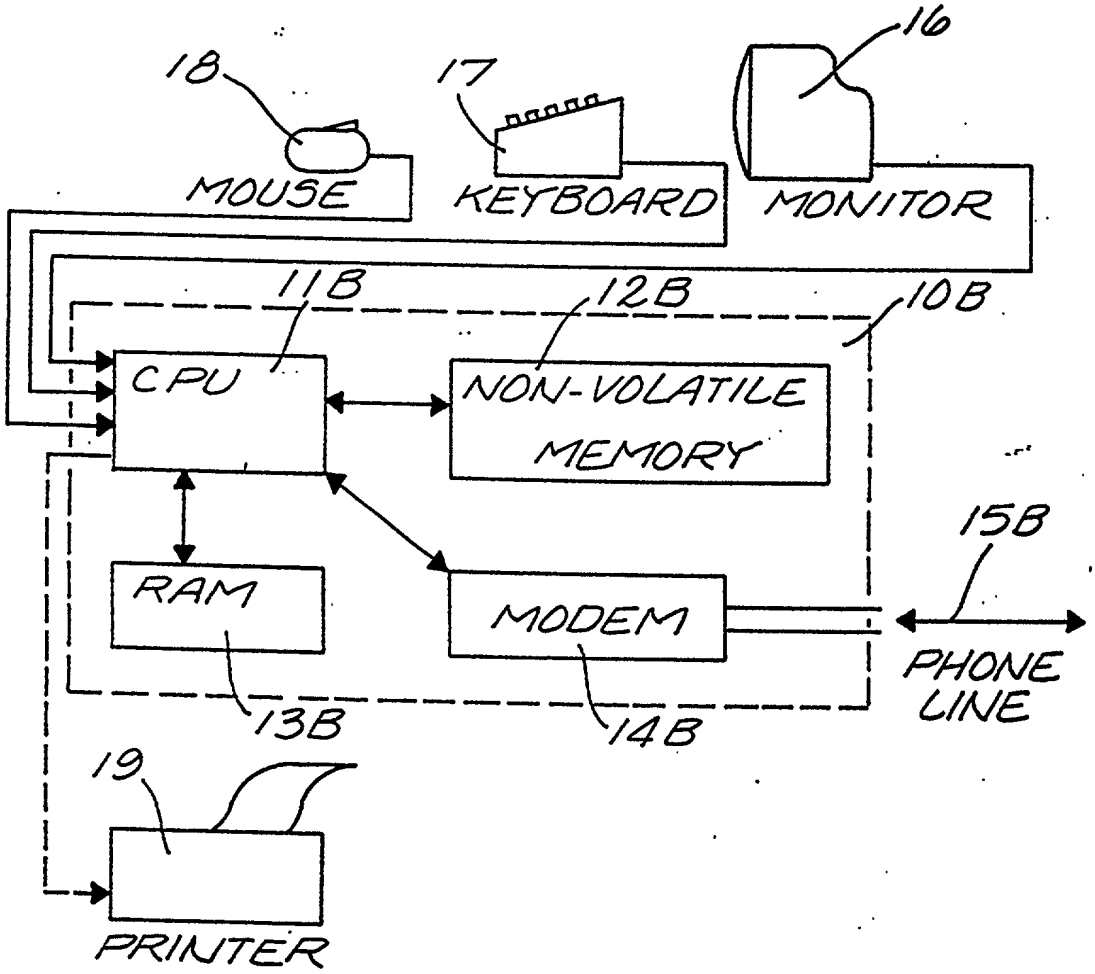

16
18
17
MOUSE
KEYBOARD
MONITOR
11B
12B
10B
CPU
NON-VOLATILE MEMORY
15B
RAM
MODEM
PHONE LINE
13B
14B
19
PRINTER

FIG. 1B

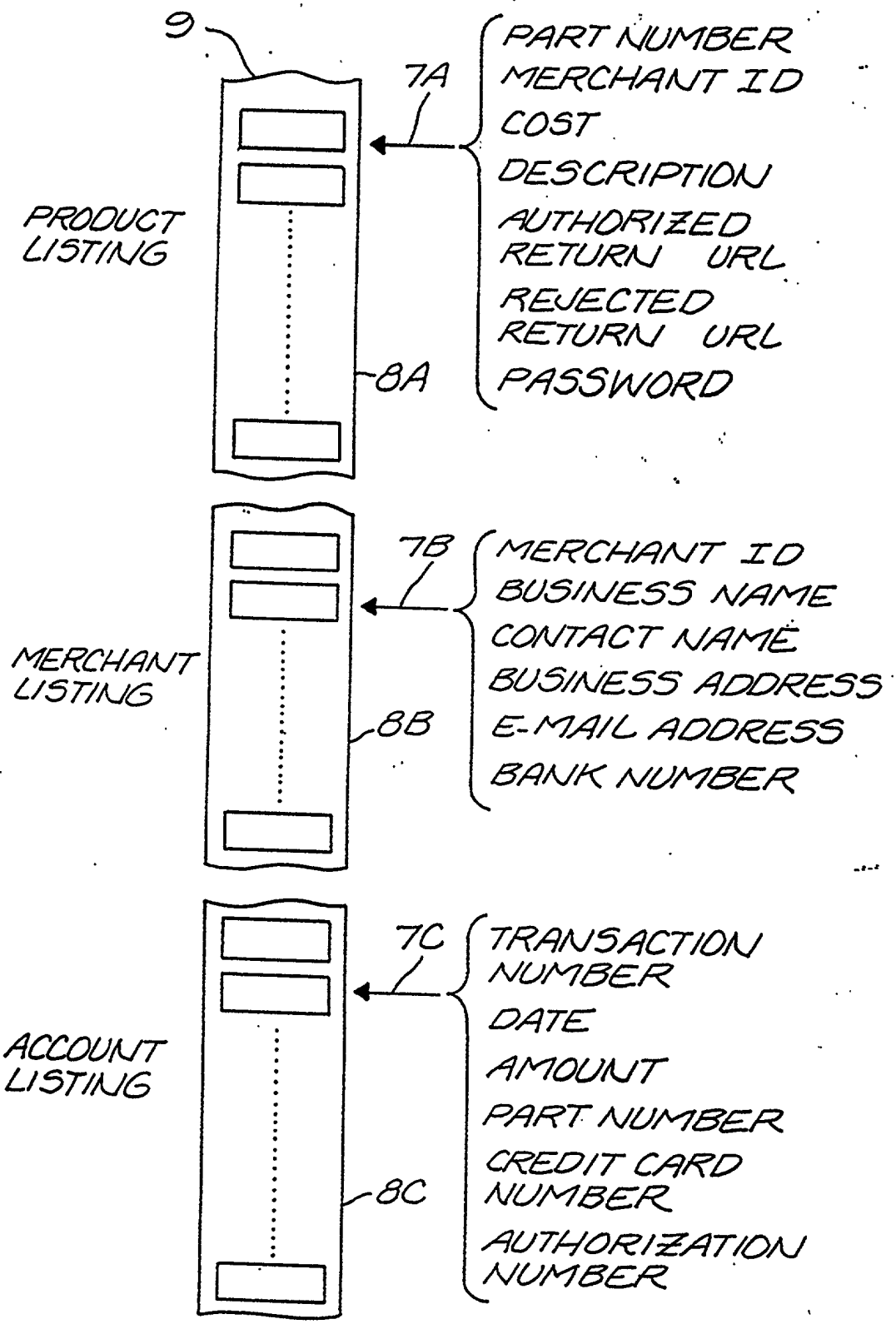

9
7A
PART NUMBER
MERCHANT ID
COST
DESCRIPTION
AUTHORIZED RETURN URL
REJECTED RETURN URL
PASSWORD
PRODUCT LISTING
8A
7B
MERCHANT ID
BUSINESS NAME
CONTACT NAME
BUSINESS ADDRESS
E-MAIL ADDRESS
BANK NUMBER
MERCHANT LISTING
8B
7C
TRANSACTION NUMBER
DATE
AMOUNT
PART NUMBER
CREDIT CARD NUMBER
AUTHORIZATION NUMBER
ACCOUNT LISTING
8C

FIG. 1C

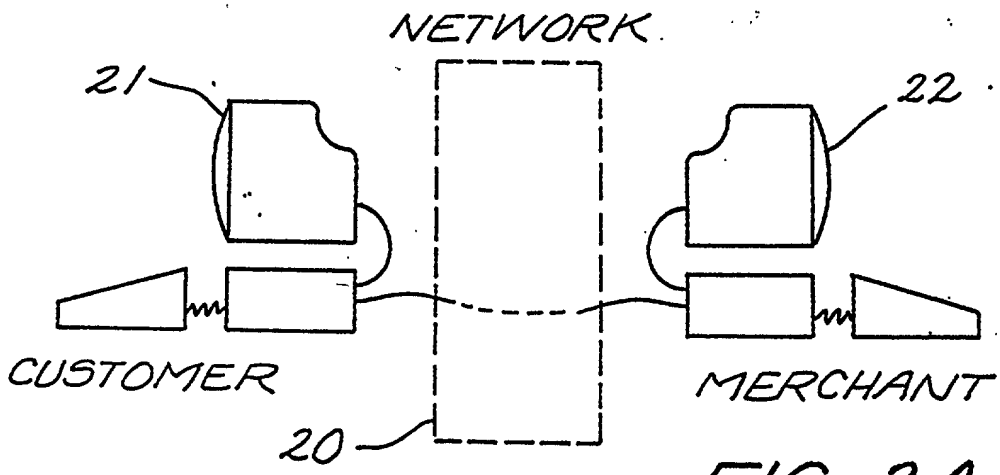


FIG. 2A

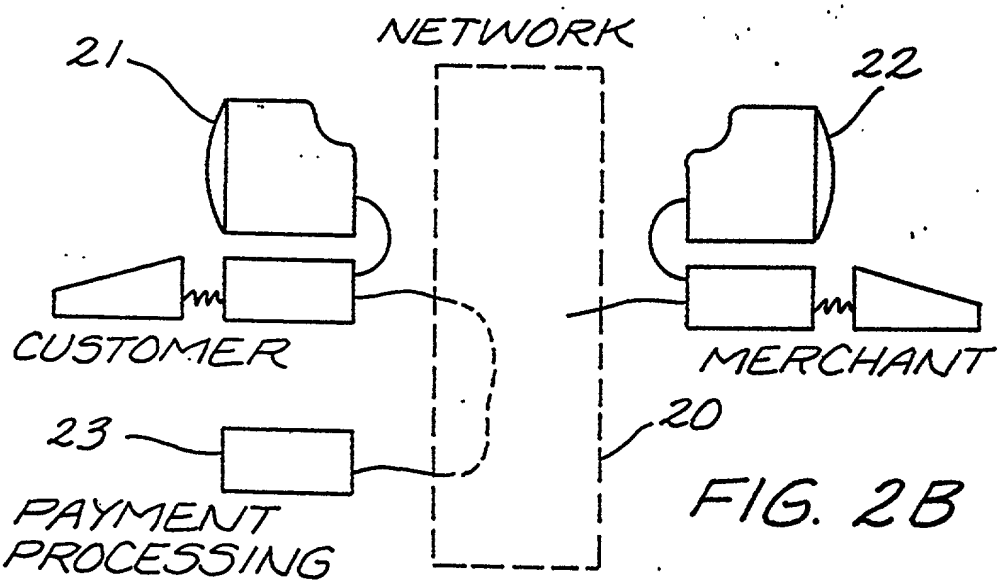


FIG. 2B

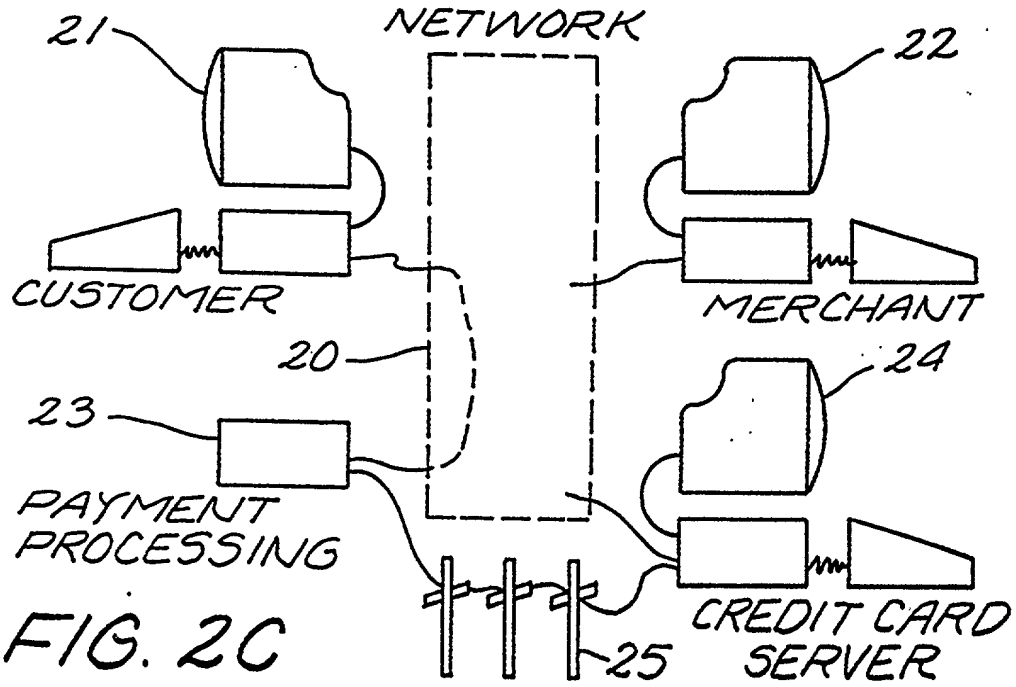


FIG. 2C

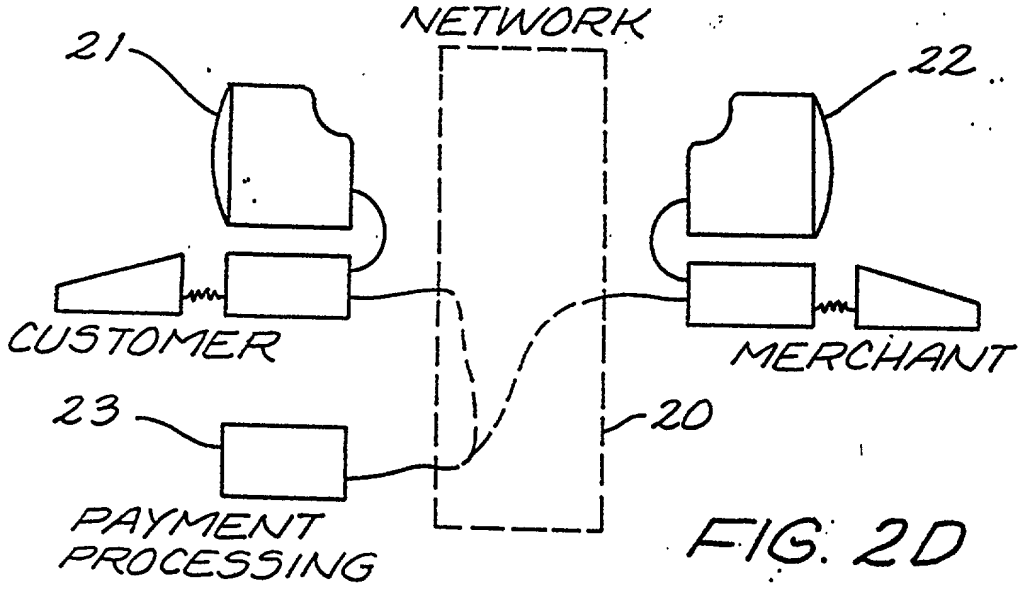
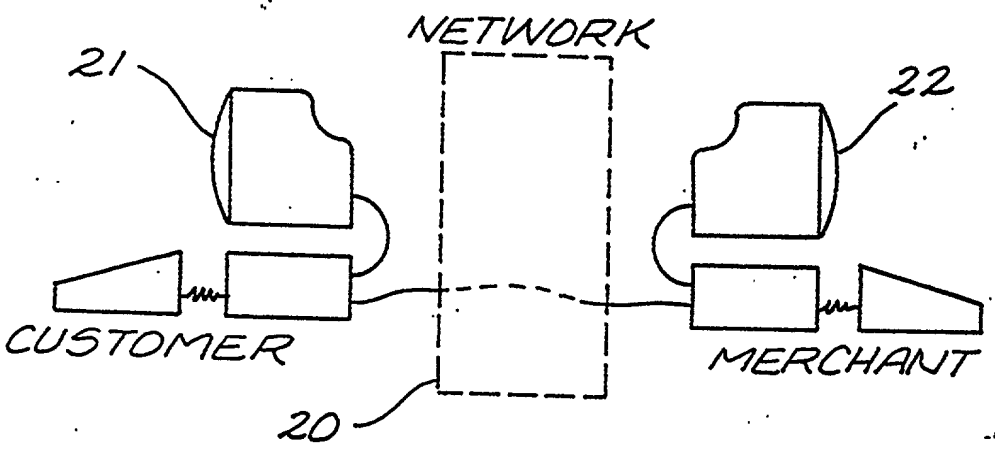

NETWORK
21
22
CUSTOMER
MERCHANT
23
20
PAYMENT
PROCESSING

FIG. 2D


NETWORK
21
22
CUSTOMER
MERCHANT
20

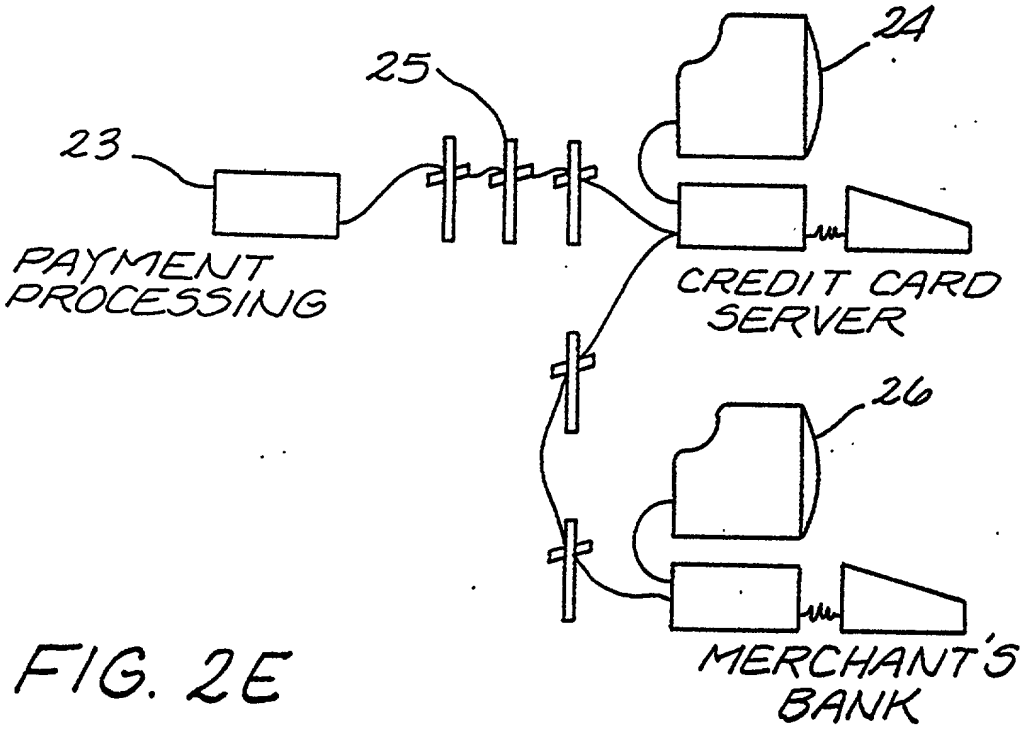

24
25
23
PAYMENT
PROCESSING
CREDIT CARD
SERVER
26
MERCHANT'S
BANK

FIG. 2E

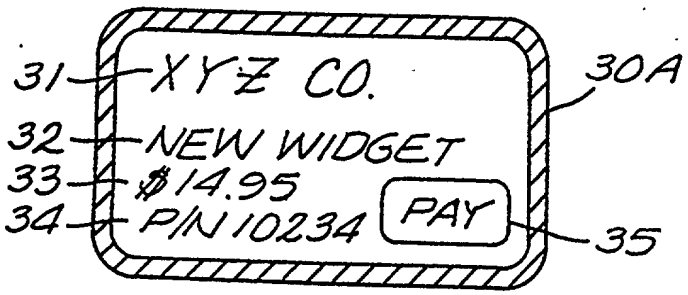


FIG. 3A

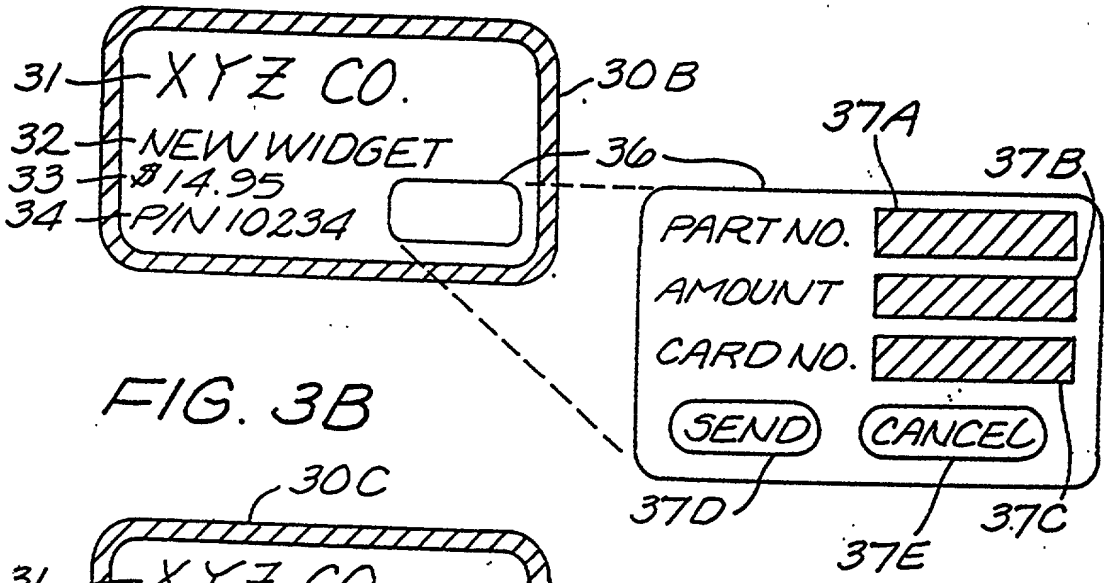


FIG. 3B

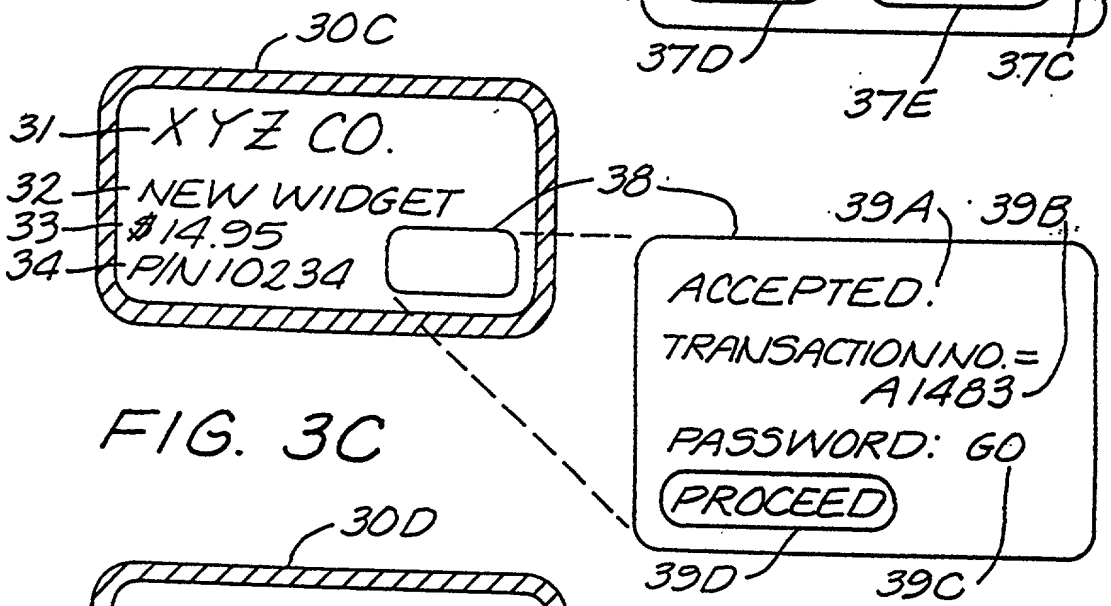


FIG. 3C

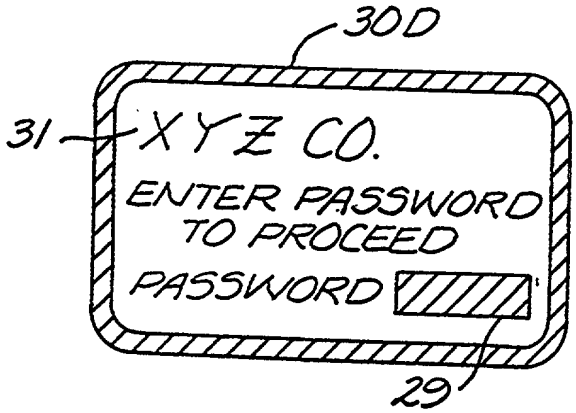


FIG. 3D

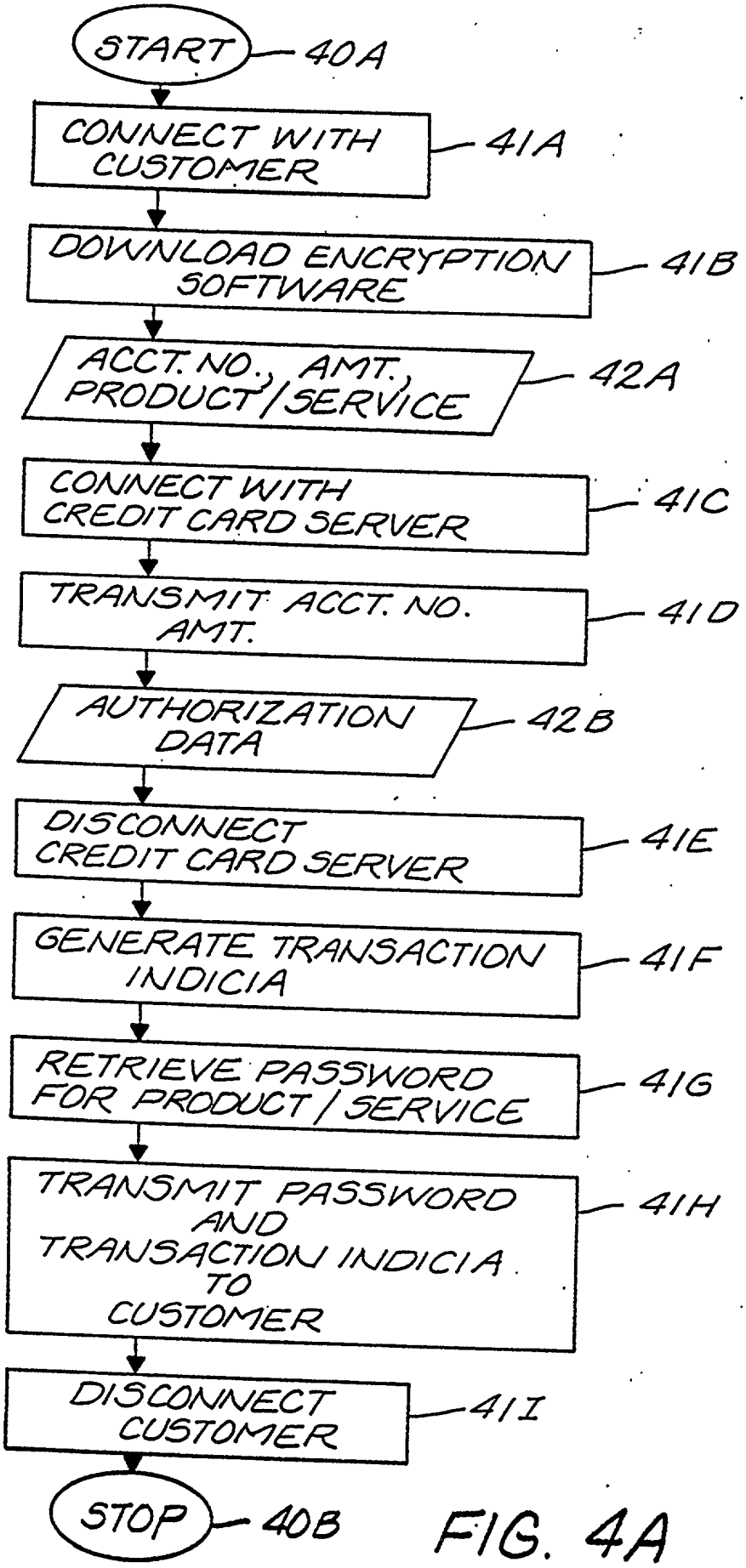
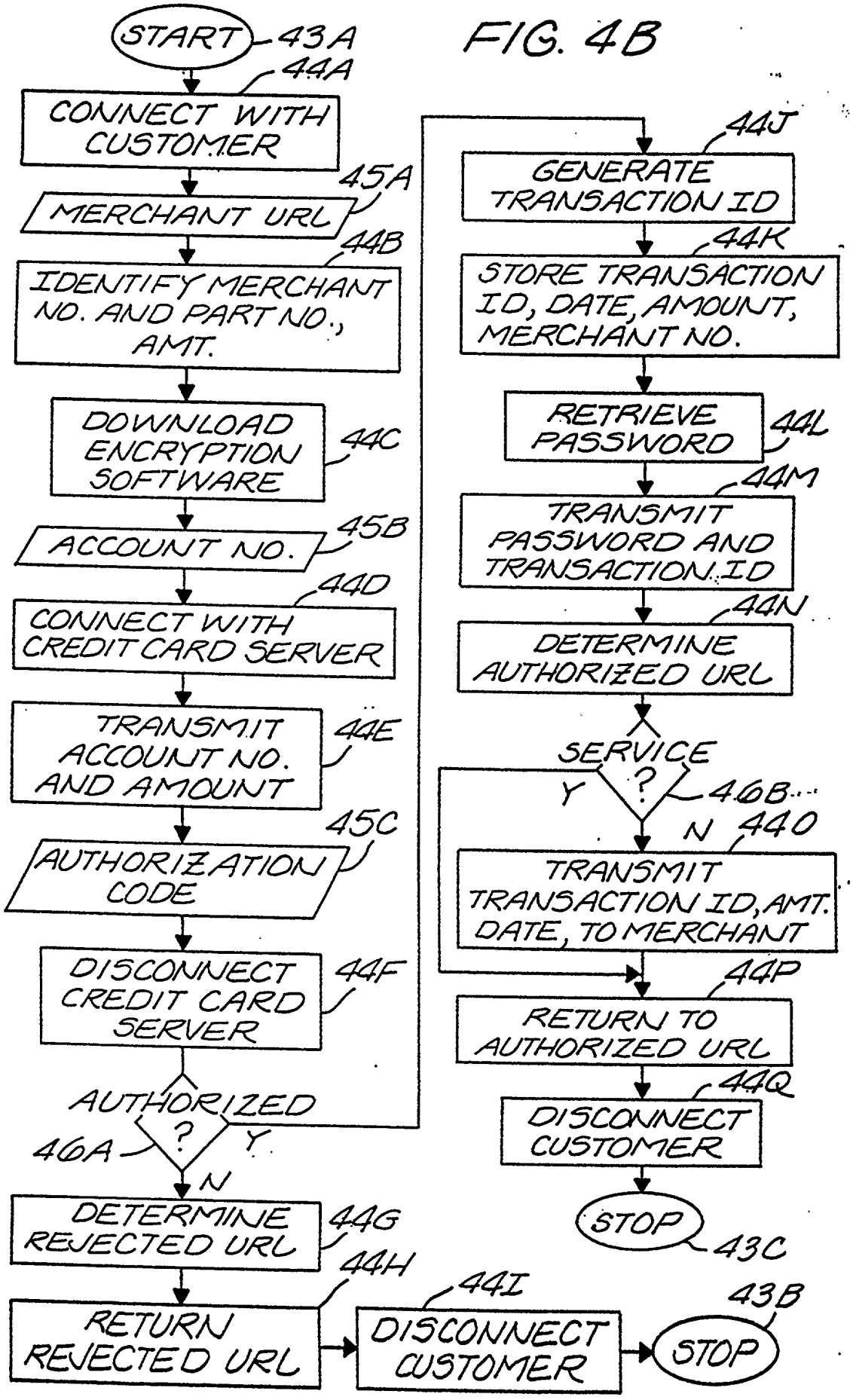

START
40A
CONNECT WITH CUSTOMER
41A
DOWNLOAD ENCRYPTION SOFTWARE
41B
ACCT. NO., AMT., PRODUCT/SERVICE
42A
CONNECT WITH CREDIT CARD SERVER
41C
TRANSMIT ACCT. NO. AMT.
41D
AUTHORIZATION DATA
42B
DISCONNECT CREDIT CARD SERVER
41E
GENERATE TRANSACTION INDICIA
41F
RETRIEVE PASSWORD FOR PRODUCT / SERVICE
41G
TRANSMIT PASSWORD AND TRANSACTION INDICIA TO CUSTOMER
41H
DISCONNECT CUSTOMER
41I
STOP
40B

FIG. 4A

FIG. 4B


START
43A
CONNECT WITH CUSTOMER
44A
MERCHANT URL
45A
IDENTIFY MERCHANT NO. AND PART NO., AMT.
44B
DOWNLOAD ENCRYPTION SOFTWARE
44C
ACCOUNT NO.
45B
CONNECT WITH CREDIT CARD SERVER
44D
TRANSMIT ACCOUNT NO. AND AMOUNT
44E
AUTHORIZATION CODE
45C
DISCONNECT CREDIT CARD SERVER
44F
AUTHORIZED ?
46A
Y
N
DETERMINE REJECTED URL
44G
RETURN REJECTED URL
44H
DISCONNECT CUSTOMER
44I
STOP
43B
GENERATE TRANSACTION ID
44J
STORE TRANSACTION ID, DATE, AMOUNT, MERCHANT NO.
44K
RETRIEVE PASSWORD
44L
TRANSMIT PASSWORD AND TRANSACTION ID
44M
DETERMINE AUTHORIZED URL
44N
SERVICE ?
46B
Y
N
TRANSMIT TRANSACTION ID, AMT. DATE, TO MERCHANT
44O
RETURN TO AUTHORIZED URL
44P
DISCONNECT CUSTOMER
44Q
STOP
43C

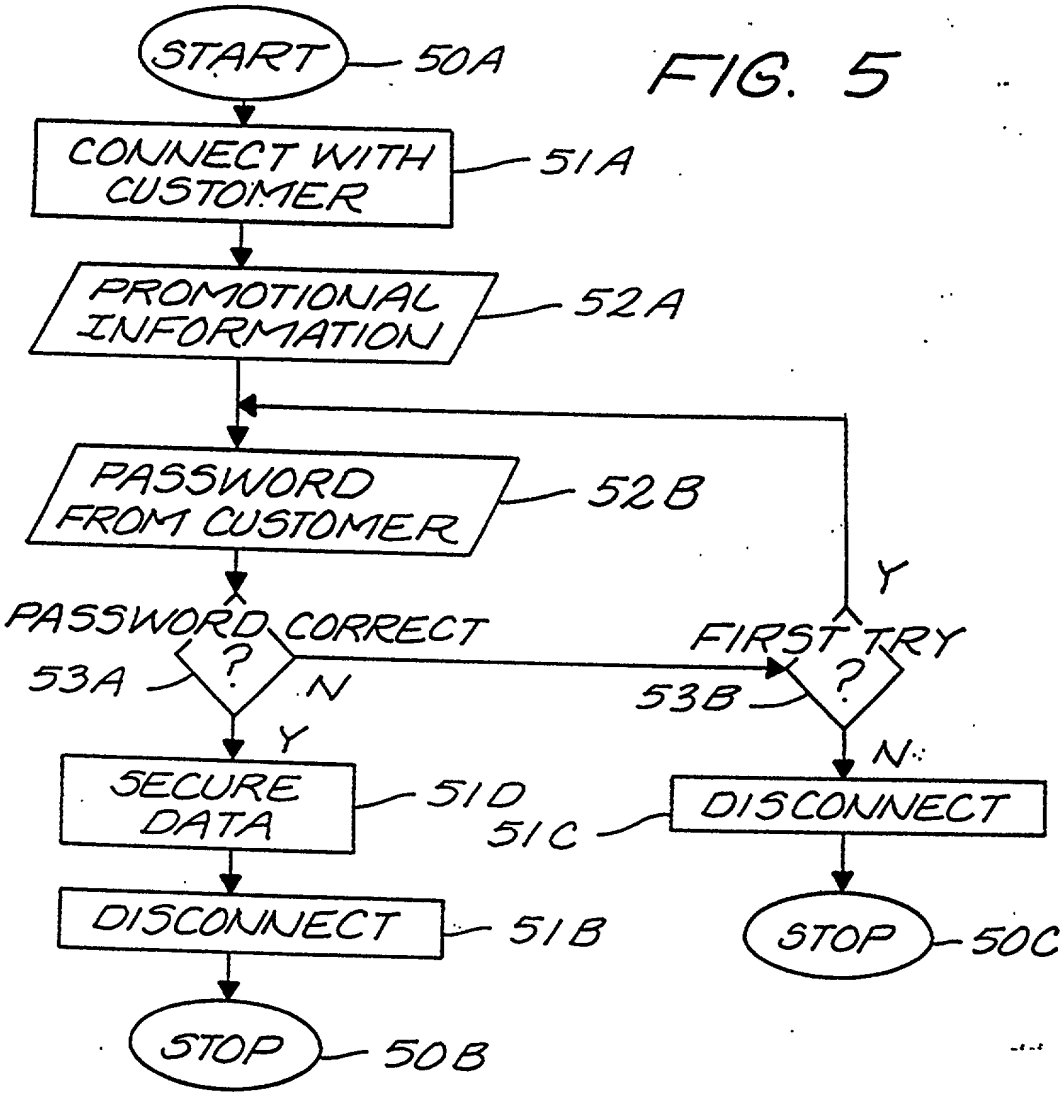

START
50A
CONNECT WITH CUSTOMER
51A
PROMOTIONAL INFORMATION
52A
PASSWORD FROM CUSTOMER
52B
PASSWORD CORRECT ?
53A
N
Y
FIRST TRY ?
53B
Y
N
SECURE DATA
51D
DISCONNECT
51B
DISCONNECT
51C
STOP
50B
STOP
50C

FIG. 5

Attorney Docket No.1475B.5.5

APPLICATION FOR U.S. PATENT
DECLARATION AND POWER OF ATTORNEY

As the below named inventor(s), I/we declare that my/our residence, post office address, and citizenship are as stated below next to my name; that I/we have read and understand the contents of the attached specification, including the claims as amended by any amendment specifically referred to herein; that I/we verily believe that I/we am/are the original, first and sole inventor(s) of the invention entitled as set forth below, which is described and claimed in the attached specification; that I/we do not know and do not believe that the same was ever known or used in the United States of America before my/our invention thereof, or patented or described in any printed prior publication in any country before my/our invention thereof, or more than one year prior to this application; or in public use or on sale in the United States of America more than one year before the date of this application; that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me/us or my/our legal representatives or assigns more than twelve months prior to this application; that no application for patent or inventor's certificate on the invention has been filed by me/us or my/our legal representative(s) or assigns in any country foreign to the United States of America; and that I/we acknowledge my duty under 37 CFR 1.56(a) to disclose information of which I/we am/are aware which is material to the examination of this application.

TITLE OF INVENTION: A METHOD OF PROCESSING PAYMENT ON A NETWORK OF COMPUTERS SUCH AS THE INTERNET

INVENTOR(S):

Full Name: Ogram (last) Mark (first) E. (middle)

Residence: 8040 S. Kolb Road (street) Tucson (city) Arizona (state) 85706 (zip)

Post Office Address: SAME AS ABOVE

Citizenship: USA

POWER OF ATTORNEY: As the named inventor(s), I/we hereby appoint the following attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

(1) Mark E. Ogram Registration No. 30343

SEND CORRESPONDENCE TO:
Mark E. Ogram, P.C.
8040 S. Kolb Road
Tucson, AZ 85706

DIRECT TELEPHONE CALLS TO:
Mark Ogram: (520) 574-3399

I/we further declare that all statements made herein of my/our own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine, or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature of Inventor(s): [signature]

Date: 9/8/00